UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,824	06/11/2001	Fengmin Gong	30540/206333	3189

7590 11/10/2004

McDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,824	GONG ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/01/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 06/11/2001. Claims 1 – 45 were received for consideration. No preliminary amendments to the claims were filed. Claims 1 – 45 are currently being considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1- 45 are rejected under 35 U.S.C. 102(e) as being anticipated by Cunningham et al. (U.S. Patent Number 6,219,786).

Regarding Claim 1, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), comprising:

a proxy server for receiving network service requests from a client and forwarding said requests pursuant to a tolerance protocol to a protected server, and responding to a client (Column 5 line 39 – Column 6 line 20);

an acceptance monitor for receiving from the protected server one or more responses to the client request and applying one or more acceptance tests thereto (Column 6 lines 1 – 25); and

a ballot monitor for receiving from the acceptance monitor the results of the applied acceptance tests and determining a preferred response to the client request (Column 6 lines 1 – 48).

Regarding Claim 2, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), comprising:

a proxy server for receiving network service requests from a client and forwarding said requests pursuant to a tolerance protocol to a protected server, and responding to a client (Column 5 line 39 – Column 6 line 20);

an acceptance monitor for receiving from the protected server one or more responses to the client request and applying one or more acceptance tests thereto (Column 6 lines 1 – 25);

a ballot monitor for receiving from the acceptance monitor the results of the applied acceptance tests and determining a preferred response to the client request (Column 6 lines 1 – 48);

an intrusion sensor responsive to anomalies in operation of the network for detecting threats to the network (Column 6 lines 21 – 56 and Column 8 lines 10 – 48); and

an adaptive reconfigurer for altering the tolerance protocol and reconfiguring a network forwarding scheme among the proxy server, acceptance monitor and ballot monitor in response to a predetermined condition (Column 6 lines 1 – 48 and Column 8 lines 26 – 53).

Regarding Claim 18, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), comprising:

receiving a network service request and forwarding the request pursuant to a tolerance protocol (Column 7 lines 1 – 14);

generating a response to the service request and forwarding the response (Column 7 lines 1 – 55);

applying one or more acceptance tests to the response and forwarding the test results (Column 7 line 56 – column 8 line 9);

polling the test results to determine a preferred response based upon the poll; and forwarding the preferred response to the client (Column 7 line 56 – Column 8 line 53).

Regarding Claim 19, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), comprising:

receiving a network service request and forwarding the request pursuant to a tolerance protocol (Column 7 lines 1 – 14);

generating a response to the service request and forwarding the response (Column 7 lines 1 – 55);

applying one or more acceptance tests to the response and forwarding the test results;

polling the acceptance test results to determine a preferred response based upon the poll; forwarding the preferred response to the client (Column 7 line 56 – column 8 line 9);

detecting any anomalies in operation of the network (Column 8 lines 34 – 53); and

revising the tolerance protocol and a network forwarding scheme in response to an anomaly in operation of the network (Column 8 line 54 – Column 9 line 13).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said proxy server further forwards said requests to an acceptance monitor and a ballot monitor (Column 6 lines 1- 32; Column 7 lines 15 – 25 and Column 8 lines 26 – 53).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said proxy server comprises multiple independent proxy servers (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said acceptance monitor comprises multiple independent acceptance monitors (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), 1 wherein said ballot monitor comprises multiple independent ballot monitors (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said proxy server forwards said requests to a protective server, the acceptance monitor and the ballot monitor (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said acceptance monitor applies one or more acceptance tests taken from the group of satisfaction of requirements test, accounting test, reasonableness test or computer run time test (Column 8 line 26 – Column 9 line 18).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), 1 wherein said ballot monitor determines a preferred response using a process taken from the group of: simple majority voting, Byzantine agreement process, or adjudication process (Column 9 line 66 – Column 11 line 48).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said proxy server forwards said requests to multiple independent protected servers (Column 5 lines 8 – 51 and Column 10 lines 21 – 51).

Claim 7 is rejected as applied above in rejecting claim 2. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said intrusion sensor comprises a multiplicity of sensors monitoring predetermined operations of the network (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 8 is rejected as applied above in rejecting claim 2. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said adaptive reconfigurer reconfigures the network forwarding scheme to establish parallel forwarding among the protected server, acceptance monitor, and ballot monitor (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 15 is rejected as applied above in rejecting claim 2. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein at least one of said proxy server, acceptance monitor, ballot monitor, intrusion sensor and adaptive reconfigurer comprise a separate and independent processor (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 16 is rejected as applied above in rejecting claim 2. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein two or more of said proxy server, acceptance monitor,

ballot monitor, intrusion sensor and adaptive reconfigurer operate on a single processor (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 17 is rejected as applied above in rejecting claim 2. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the adaptive reconfigurer reconfigures the network forwarding scheme to establish multiple independent network forwarding paths (Column 6 lines 1 – 32 and Column 8 line 26 – Column 9 line 48).

Claim 20 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of receiving a network service request further comprises receiving a network service request at a proxy server (Column 6 lines 1 – 32).

Claim 21 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of receiving a network

service request further comprises forwarding the request to multiple protected servers (Column 6 lines 1 – 32).

Claim 22 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of receiving a network service request further comprises forwarding the request to multiple protected servers (Column 5 lines 8 – 51 and Column 10 lines 21 – 52).

Claim 23 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of receiving a network service request further comprises forwarding the request on multiple independent paths (Column 6 lines 1 – 32 and Column 8 line 26 – Column 9 line 48).

Claim 24 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of generating a response comprises generating a response at a protected server (Column 6 lines 1 – 32).

Claim 25 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of generating a response and forwarding the response comprises forwarding a response to an acceptance monitor (Column 6 lines 1- 32; Column 7 lines 15 – 25 and Column 8 lines 26 – 53).

Claim 26 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of generating a response and forwarding a response comprises forwarding the response to multiple acceptance monitors (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 27 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of generating a response and forwarding a response comprises forwarding the response on multiple independent paths (Column 6 lines 1 – 32 and Column 8 line 26 – Column 9 line 48).

Claim 28 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of applying one or more acceptance tests comprises applying one or more acceptance tests at an acceptance monitor (Column 8 line 26 – Column 9 line 18).

Claim 29 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of applying one or more acceptance tests comprises applying independent acceptance tests to each response (Column 8 line 26 – Column 9 line 18).

Claim 30 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of applying one or more acceptance tests and forwarding the test results comprises forwarding the test results to a ballot monitor (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 31 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of applying one or more acceptance tests and forwarding the test results comprises forwarding the tests results to multiple ballot monitors (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 32 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of applying one or more acceptance tests and forwarding the test results comprises forwarding the tests results on multiple independent paths (Column 6 lines 1 – 32 and Column 8 line 26 – Column 9 line 48).

Claim 33 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of polling the acceptance test results comprises polling the acceptance test results at a ballot monitor (Column 6 lines 1 – 32 and Column 7 line 56 – Column 8 line 53).

Claim 34 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of polling the acceptance test results comprises applying multiple polling routines (Column 6 lines 1 – 32 and Column 7 line 56 – Column 8 line 53).

Claim 35 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of polling the acceptance test results comprises applying multiple polling routines to the responses from each of a multiplicity of ballot monitors (Column 6 lines 1 – 32 and Column 7 line 56 – Column 8 line 53).

Claim 36 is rejected as applied above in rejecting claim 18. Furthermore, Cunningham teaches and describes a method for reconfiguring communication among network components to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein at least one of the steps of receiving a network service request, generating a response to a service request, applying one or more acceptance tests, polling the acceptance test results and forwarding the preferred response to a client comprises utilizing a separate processor to enhance

independence of operation and minimize the impact of intrusive events (Column 7 line 56 – Column 8 line 53).

Claim 37 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding on multiple independent paths (Column 6 lines 1 – 32 and Column 8 line 26 – Column 9 line 48).

Claim 38 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding to multiple independent acceptance monitors (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 39 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to

minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding to multiple independent ballot monitors (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 40 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding to multiple independent proxy servers (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 41 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme further comprises comparing any detected anomalies with known anomalies to identify a predetermined intrusion tolerance protocol (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 42 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme comprises determining the acceptance monitors that will be used to support the selected tolerance protocol (Column 8 line 54 – Column 9 line 48).

Claim 43 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme comprises determining the ballot monitors that will be used to support the selected tolerance protocol (Column 8 line 54 – Column 9 line 48).

Claim 44 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network

forwarding scheme comprises determining the proxy servers that will be used to implement the selected tolerance protocol (Column 8 line 54 – Column 9 line 48).

Claim 45 is rejected as applied above in rejecting claim 19. Furthermore, Cunningham teaches and describes a method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein the step of revising the tolerance protocol and network forwarding scheme comprises prioritizing the network service requests (Column 8 line 54 – Column 9 line 48 and Column 10 line 32 – Column 11 line 46).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said acceptance monitor receives responses from multiple independent protected servers and applies independent acceptance tests to each received responses (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Cunningham teaches and describes a dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to

minimize the impact of intrusive events (Fig. 1, 2, 6 7; Summary and Column 5 line 8 – Column 11 line 50), wherein said ballot monitor receives responses from multiple acceptance monitors and determines a preferred response from the multiple responses received (Column 6 lines 1 – 32 and Column 8 lines 26 – 53).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

November 04, 2004.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100